UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,501	11/02/2000	Oleg Rashkovskiy	042390.P10142	8091

21906 7590 12/08/2006

TROP PRUNER & HU, PC
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/706,501	RASHKOVSKIY ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28,56-76,79-81 and 91-96* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28, 56-76, 79-81, and 91-96* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Reopening of Prosecution - New Ground of Rejection After Appeal Brief

In view of the Appeal Brief filed on 9/24/2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-28, 56-76, 79-81, and 91-96 are rejected under 35 U.S.C. 103(a) as being unpatentable over Etzel et al., (U.S. Patent No. 6,577,734 and Etzel hereinafter), in view of Doland, (U.S. Patent No. 6,415,032).

Regarding claim 1, Etzel discloses an apparatus comprising:

a key generator for generating a key according to an identifier value of another apparatus (i.e., modules 30, 50, and 215 each independently generate a symmetrical encryption key, also "client variable", using **the other module's public key** and its own private key wherein the other module has generated its public key by applying a one-way function to the private key which is a device unique key)(col. 4, lines 35-67 and col. 5, lines 1-4 – wherein in col. 8, lines 5, it is expressly disclosed that the public key of each chip/module is stored as a serial number in a database).

Although Etzel discloses encryption and decryption of content (i.e., the program key) using a respective symmetrical key which is unique to the pair of chips/modules as a result of the public key associated with the sending module (col. 5, lines 1-5 and col. 7, lines 61-67 and col. 8, lines 1-5), it does not disclose reordering the blocks of an original content item according to the generated symmetrical key.

However, Doland discloses a reorderer for reordering the blocks of an original content item (i.e., bit position permutation) according to a symmetrical key K (col. 8, lines 25-54).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the encryption system of Etzel by including

reordering the blocks of an original content item as disclosed by Doland. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doland to provide for encrypting a message by performing a bit position permutation on one or more message blocks (Doland, Col. 3, lines 20-61).

Regarding claim 56, Etzel discloses an apparatus comprising:

a server (i.e., video server) including, a stored copy of a client identifier (i.e., the address of the requesting terminal)(col. 7, lines 45-60);

a key generator for generating a symmetrical encryption key according to the copy of the client identifier, and means for transmitting a content item (i.e., the program key) to a client in an encrypted format according to the symmetrical encryption key (i.e., modules 50 and 215 each independently generate a symmetrical encryption key, also "client variable", using **the other module's public key** and its own private key wherein the other module has generated its public key by applying a one-way function to the private key which is a device unique key)(col. 4, lines 35-67 and col. 5, lines 1-4 - wherein in col. 8, lines 5, it is expressly disclosed that the public key of each chip/module is stored as a serial number in a database); and

the client (i.e., ACS 40) including, the client identifier, client storage for storing the encrypted content item, and means for accessing the content item from the client storage in an original decrypted format (col. 6, lines 23-46).

Although Etzel discloses encryption and decryption of content (i.e., the program key) using a respective symmetrical key which is unique to the pair of chips/modules as a result of the public key associated with the sending module (col. 5, lines 1-5 and col. 7, lines 61-67 and col. 8, lines 1-5), it does not disclose reordering the blocks of an original content item according to the generated symmetrical key.

However, Doland discloses a reorderer for reordering the blocks of an original content item (i.e., bit position permutation) according to a symmetrical key K (col. 8, lines 25-54).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the encryption system of Etzel by including reordering the blocks of an original content item as disclosed by Doland. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doland to provide for encrypting a message by performing a bit position permutation on one or more message blocks (Doland, Col. 3, lines 20-61).

Regarding claims 79-81, Etzel discloses a method of transmitting an original content item from a first entity (i.e., module 50) to a second entity (i.e., module 215) which has an identifier value, comprising:

generating a key as a function of the identifier value (i.e., the public key of the other chip/module), reordering (i.e., encrypting) blocks of the original content item as a function of the key, to create a reordered (i.e., encrypted) content item, delivering the

reordered (i.e., encrypted) content item to the second entity (i.e., chip/module 215)(col. 5, lines 35-67 and col. 6, lines 1-43);

creating a block reordering structure within the second entity (i.e., security module 215), and accessing a block of the original content item by retrieving it from the reordered (i.e., encrypted) content item according to the block reordering structure (i.e., security module 215 then uses the decrypted shared key to decrypt the program key/content item associated with the program requested by the subscriber)(col. 7, lines 34-45).

Although Etzel discloses encryption and decryption of content (i.e., the program key) using a respective symmetrical key which is unique to the pair of chips/modules as a result of the public key associated with the sending module (col. 5, lines 1-5 and col. 7, lines 61-67 and col. 8, lines 1-5), it does not disclose reordering the blocks of an original content item according to the generated symmetrical key.

However, Doland discloses a reorderer for reordering the blocks of an original content item (i.e., bit position permutation) according to a symmetrical key K (col. 8, lines 25-54).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the encryption system of Etzel by including reordering the blocks of an original content item as disclosed by Doland. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doland to provide for encrypting a message

by performing a bit position permutation on one or more message blocks (Doland, Col. 3, lines 20-61).

Regarding claim 91, Etzel discloses a recordable medium having recorded thereon a reordered content item resulting from the process comprising:

generating a key in response to an identifier value of a content retrieval entity col. 4, lines 35-67 and col. 5, lines 1-4 -wherein in col. 8, lines 5, it is expressly disclosed that the public key of each chip/module is stored as a serial number in a database); and

reordering (i.e., encrypting), as controlled by the key, blocks of an original content item to create the reordered (i.e., encrypted) content item (i.e., security module 215 then uses the decrypted shared key to decrypt the program key/content item associated with the program requested by the subscriber)(col. 7, lines 34-45).

Although Etzel discloses encryption and decryption of content (i.e., the program key) using a respective symmetrical key which is unique to the pair of chips/modules as a result of the public key associated with the sending module (col. 5, lines 1-5 and col. 7, lines 61-67 and col. 8, lines 1-5), it does not disclose reordering the blocks of an original content item according to the generated symmetrical key.

However, Doland discloses a reorderer for reordering the blocks of an original content item (i.e., bit position permutation) according to a symmetrical key K (col. 8, lines 25-54).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the encryption system of Etzel by including

reordering the blocks of an original content item as disclosed by Doland. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doland to provide for encrypting a message by performing a bit position permutation on one or more message blocks (Doland, Col. 3, lines 20-61).

Regarding claims 2-4 and 57-59, Etzel discloses the apparatus of claim 1 further comprising: a transmitter to distribute the reordered blocks over a wireless broadcast channel (page 1, lines 10-16).

Regarding claims 5-6, Etzel discloses further comprising: means for writing the reordered (i.e., encrypted) blocks to a removable storage disc (i.e., the subscriber terminal stores the program encryption key, i.e., the content item, which is still protected by the key shared with ACS 40, in memory until the associated user enters signals – wherein the memory can be any storage including removable storage disc)(col. 7, lines 23-33).

Regarding claims 7 and 60, Etzel does not expressly disclose wherein each of the reordered blocks comprises a same data content as its corresponding block from the original content item.

However, Doland discloses wherein each of the reordered blocks comprises a same data content as its corresponding block from the original content item (i.e., during

bit position and bit pattern permutations, values, within the array A, being denoted as v(i)- where i=0,...,n-1- are used to swap around bits in a message block in a controlled and a reproducible fashion – wherein after the permutation, the data content of each message block remains the same as its corresponding message block before the permutation)(col. 8, lines 25-67 and col. 9, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the encryption system of Etzel by including wherein each of the reordered blocks comprises a same data content as its corresponding block from the original content item as disclosed by Doland. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doland to provide for encrypting a message by performing a bit position permutation on one or more message blocks (Doland, Col. 3, lines 20-61).

Regarding claims 8-9 and 61-62, Etzel does not expressly disclose wherein the reordered blocks are of any block sizes.

However, Doland discloses wherein the reordered blocks are of any block sizes (col. 8, lines 33-53).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the encryption system of Etzel by including wherein the reordered blocks are of any block sizes as disclosed by Doland. This modification would have been obvious because one of ordinary skill in the art would

have been motivated by the suggestion of Doland to provide for encrypting a message by performing a bit position permutation on one or more message blocks (Doland, Col. 3, lines 20-61).

Regarding claims 10-11 and 63, Etzel discloses further comprising: means for keeping a list of identifier values of a plurality of such other apparatuses, wherein, for different identifier values of two such other apparatuses, the key generator generates different keys, and wherein, in response to the different keys, the reorderer imposes different new block orders on the original content item (i.e., a respective symmetrical key is unique to the pair of module as a result of the public key associated with the receiving module/module 215)(col. 4, lines 55-67 and col. 5, lines 1-7 and col. 6, lines 19-42).

Regarding claim 12, Etzel discloses wherein:

the list includes a first identifier value for a first such other apparatus, and a second identifier value for both a second and a third such other apparatus, wherein the second identifier value is different than the first identifier value (i.e., CV is a function of the address of the associated subscriber terminal)(col. 6, lines 3-42), and the reorderer (i.e., server 60) imposes a first new block order on the original content item for distribution to the first such other apparatus, and a second, different new block order on the original content item for distribution to either the second or the third such other apparatus (col. 6, lines 46-67 and col. 7, lines 45-67).

Regarding claims 13-16, 65-68, and 94-96, Etzel discloses wherein the identifier value is a serial number of the other apparatus (col. 4, lines 38-55 and col. 8, lines 5-17).

Regarding claim 17, Etzel discloses wherein: the apparatus is a server, the other apparatus is one of a plurality of clients, and the server further comprises, means for provisioning the clients, including the selection of the identifier values for the clients (i.e., only the terminals whose address is contained in the message "reads in" the message), and means for maintaining a list of the clients' identifier values (i.e., module 215 locates the program id in the message, associates that id with the proper key-cache memory location, unloads the program encryption key stored at that memory location, and uses the key to decrypt the program segment contained in the received message)(col. 7, lines 45-67 and col. 8, lines 1-5).

Regarding claim 18, Etzel discloses the apparatus of claim 1 wherein the identifier value comprises the session key (col. 6, lines 6-23).

Regarding claims 19-20, and 69-70, Etzel discloses discloses further comprising:

a transmitter for communicating over a key channel and a content channel (i.e., wherein the bi-directional communication path 41 and the uni-direction path 61 are the

physical channels including the virtual channels for transmitting key and content)(col. 7, lines 4-6 and lines 45-61).

Regarding claims 21-26, and 71-76, Etzel discloses wherein the original content item comprises an electronic programming guide (i.e., the identity of the program or the program id)(col. 7, lines 45-61).

Regarding claim 64, Etzel discloses further comprising: two or more distinct pluralities of such clients, a plurality of such servers, each in communication with a respective distinct plurality of such clients, and each respective server's means for transmitting being configured to reorder (i.e., encrypt) blocks of the content item in an order which is re-orderable (i.e., capable of being decrypted) only by the plurality of clients with which that respective server is in communication (col. 8, lines 5-26).

Regarding claim 27, Etzel does not expressly disclose reordering blocks of the original content item and storing them to the storage device according to a logical addressing system of the apparatus.

However, Doland discloses wherein the reorderer reorders blocks of the original content item and stores them to the storage device according to a logical addressing system of the apparatus (col. 8, lines 25-67 and col. 9, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the encryption system of Etzel by including

wherein the reorderer reorders blocks of the original content item and stores them to the storage device according to a logical addressing system of the apparatus as disclosed by Donald. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Donald to provide for encrypting a message by performing a bit position permutation on one or more message blocks (Donald, Col. 3, lines 20-61).

Regarding claim 28, Etzel does not expressly disclose reordering blocks of the original content item and storing them to the storage device according to a logical addressing system of the apparatus.

However, Doland discloses wherein the reorderer reorders blocks of the original content item by directly manipulating physical addresses at which the blocks are stored to the storage device (col. 8, lines 25-67 and col. 9, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the encryption system of Etzel by including wherein the reorderer reorders blocks of the original content item by directly manipulating physical addresses at which the blocks are stored to the storage device as disclosed by Doland. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Doland to provide for encrypting a message by performing a bit position permutation on one or more message blocks (Doland, Col. 3, lines 20-61).

Regarding claim 92, Etzel discloses the recordable medium of claim 91 wherein the reordered content item results from the process further comprising: the process being performed in a server, and the content retrieval entity being one of a plurality of clients connectable to the server, and the server maintaining a list of respective identifier values of the clients (col. 6, lines 19-42 and col. 7, lines 7-28).

Regarding claim 93, Etzel discloses the recordable medium of claim 92 wherein the reordered content item results from the process further comprising: the server creating the respective identifier values of the clients to be mutually unique (i.e., a respective symmetrical key is unique to the pair of module as a result of the public key associated with the receiving module/module 215)(col. 4, lines 55-67 and col. 5, lines 1-7).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Arezoo Sherkat
Patent Examiner
Group 2131
Dec. 6, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100